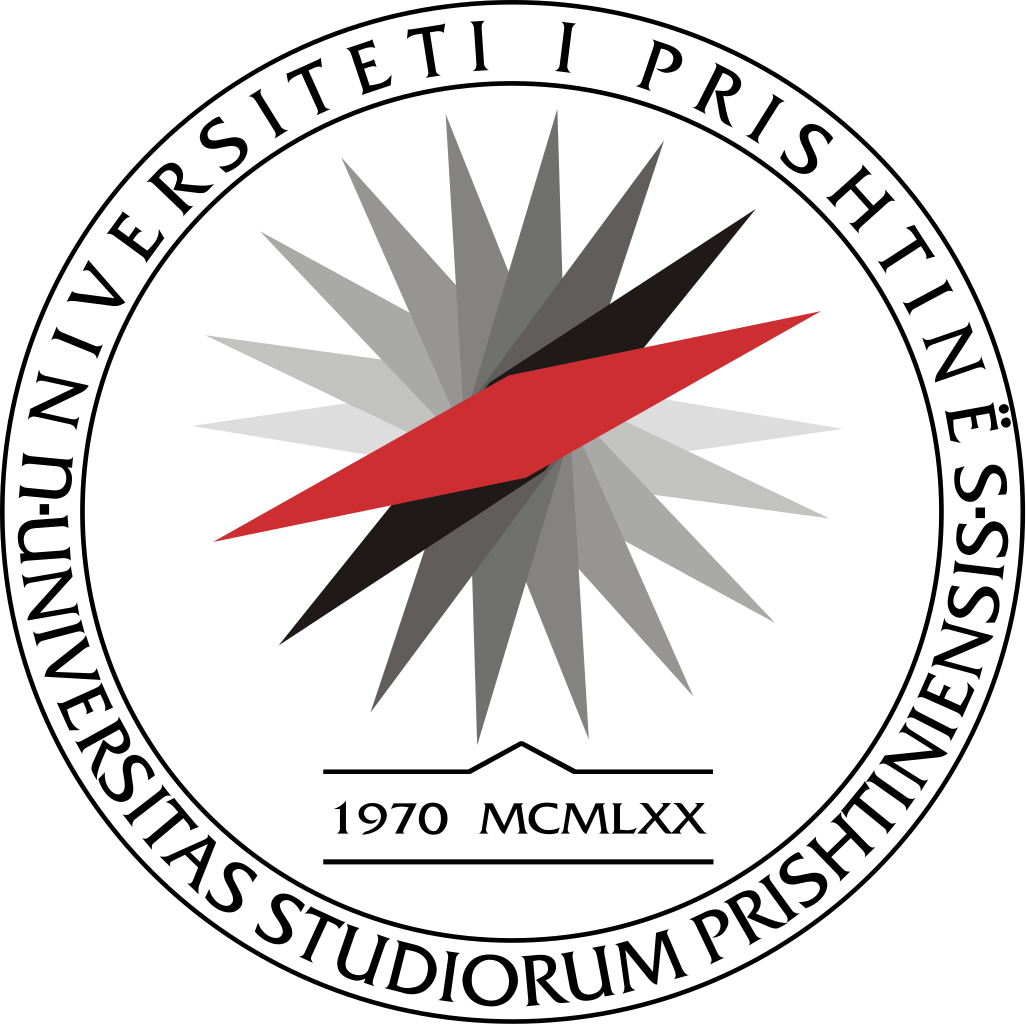
**UNIVERSITETI I PRISHTINËS**

**FAKULTETI I SHKENCAVE MATEMATIKE – NATYRORE**

**DEPARTAMENTI I MATEMATIKËS**

**PROGRAMI: Shkencë Kompjuterike**



Lënda: Siguria e te dhenave

Tema: Shifra Vegenere

Studentët:

* Lisa Ramizi

# Abstrakti

Shifra Vigenère është një teknikë klasike e kriptimit që ka luajtur një rol të rëndësishëm në fushën e kriptografisë. Zhvilluar në shekullin e 16-të nga Giovan Battista Bellaso, ky shifër zëvendësimi polialfabetik ka intriguar kriptanalistë dhe studiues për shekuj me radhë. Ky dokument kërkimor ofron një përmbledhje historike gjithëpërfshirëse të shifrës Vigenère, duke theksuar origjinën, përparimet dhe kontributet e dukshme në fushën e kriptimit. Për më tepër, punimi paraqet një analizë të thellë të zbatimit të shifrës Vigenère, duke u fokusuar në algoritmin e tij, gjenerimin e çelësave dhe konsideratat e sigurisë. Duke kuptuar historinë dhe aspektet teknike të shifrës Vigenère, studiuesit mund të vlerësojnë pikat e forta dhe të dobëta të tij, duke hapur rrugën për përparime të mëtejshme në fushën e kriptografisë moderne.

# Hyrje

Kriptografia, arti i komunikimit të sigurt, ka qenë një aspekt themelor i qytetërimit njerëzor për shekuj. Nga kohët e lashta deri në epokën dixhitale, nevoja për të mbrojtur informacionin e ndjeshëm nga aksesi i paautorizuar ka nxitur zhvillimin e teknikave të ndryshme të enkriptimit. Ndër këto teknika, shifra Vigenère, një shifër zëvendësimi polialfabetik, zë një vend të spikatur në historinë e kriptografisë. Shifra Vigenère, e shpikur nga Giovan Battista Bellaso në shekullin e 16-të, revolucionarizoi fushën e kriptimit duke prezantuar konceptin e zëvendësimit polialfabetik. Ndryshe nga paraardhësi i tij, shifra e Cezarit, e cila përdorte një model zëvendësimi fiks, shifra Vigenère prezantoi një model zëvendësimi të ndryshueshëm bazuar në një çelës sekret. Kjo risi e bëri shifrën Vigenère dukshëm më rezistente ndaj sulmeve të analizës së frekuencës, të cilat zakonisht përdoreshin për të thyer shifrat e mëparshme. Gjatë gjithë ekzistencës së tij, shifra Vigenère ka shërbyer jo vetëm si një mjet për enkriptim, por gjithashtu ka magjepsur kriptanalistët dhe studiuesit me kompleksitetin dhe vetitë e tij intriguese. Gjatë viteve, janë bërë përpjekje të shumta për të analizuar dhe thyer shifrën Vigenère, duke çuar në zhvillimin e teknikave të reja të kriptanalizës dhe duke hedhur themelet për metodat moderne të kriptimit. Ky punim kërkimor synon të ofrojë një pasqyrë gjithëpërfshirëse historike të shifrës Vigenère, duke hedhur dritë mbi origjinën, përparimet dhe kontributet e rëndësishme në fushën e kriptimit. Duke u thelluar në detajet algoritmike dhe aspektet e zbatimit të shifrës Vigenère, ky punim kërkon gjithashtu të analizojë pikat e forta, dobësitë dhe konsideratat e sigurisë. Të kuptuarit e kontekstit historik dhe ndërlikimeve teknike të shifrës Vigenère është thelbësore për studiuesit dhe kriptografët. Duke studiuar këtë teknikë klasike të kriptimit, studiuesit mund të fitojnë njohuri mbi evolucionin e kriptografisë dhe të shfrytëzojnë mësimet e nxjerra për të avancuar algoritmet moderne të kriptimit. Për më tepër, analizimi i detajeve të zbatimit të shifrës Vigenère mund të ndihmojë në kuptimin e karakteristikave të performancës, kompleksitetit dhe përdorimit të mundshëm të tij në aplikacionet kriptografike bashkëkohore. Duke eksploruar rëndësinë historike, detajet algoritmike dhe aspektet e zbatimit të shifrës Vigenère, ky punim kërkimor synon të kontribuojë në tërësinë e njohurive në fushën e kriptografisë. Në fund të fundit, një kuptim më i thellë i shifrës Vigenère mund të hapë rrugën për teknikat e përmirësuara të kriptimit dhe të rrisë sigurinë e informacionit në epokën dixhitale.

# Historiku

Shifra Vigenère, e quajtur sipas krijuesit të saj Giovan Battista Bellaso, u shfaq gjatë periudhës së Rilindjes në shekullin e 16-të. Ndërsa Bellaso shpesh atribuohet si shpikësi i shifrës Vigenère, zhvillimi i tij u ndërtua mbi teknikat dhe idetë e mëparshme të kriptimit. Shifra Vigenère përfaqësoi një përparim të rëndësishëm në kriptim, duke prezantuar konceptin e zëvendësimit polialfabetik. Përpara shifrës Vigenère, shifra e Cezarit përdorej gjerësisht për kriptim. Shifra e Cezarit, që i atribuohet Jul Cezarit, përfshinte zhvendosjen e çdo shkronje të tekstit të thjeshtë me një numër të caktuar pozicionesh në alfabet. Sidoqoftë, shifra e Cezarit ishte e ndjeshme ndaj sulmeve të analizës së frekuencës, pasi modeli i zëvendësimit mbeti konstant në të gjithë tekstin e shifruar. Bellaso u përpoq të kapërcejë cenueshmërinë e shifrës së Cezarit duke futur ndryshueshmëri në modelin e zëvendësimit. Shifra Vigenère e arriti këtë duke përdorur alfabete të shumta, secili i zhvendosur nga një shkronjë e ndryshme kryesore. Zgjedhja e çelësit përcaktoi modelin specifik të zëvendësimit të aplikuar gjatë kriptimit dhe deshifrimit, duke e bërë atë rezistent ndaj metodave tradicionale të analizës së frekuencës. Shifra Vigenère fitoi popullaritet dhe pa një përdorim të dukshëm historik. Ai u miratua nga subjekte të ndryshme ushtarake dhe diplomatike si një mjet komunikimi të sigurt. Për shembull, gjatë Luftës Civile Amerikane, si forcat e Bashkimit ashtu edhe ato të Konfederatës përdorën shifrën Vigenère për të mbrojtur informacionin e ndjeshëm. Ky përdorim tregoi vlerën praktike dhe efektivitetin e shifrës gjatë kohërave të konfliktit dhe spiunazhit. Pavarësisht suksesit të tij fillestar, kriptanalistët nuk u penguan nga përpjekjet për të thyer shifrën Vigenère. Në shekullin e 19-të, u bënë përparime të dukshme në teknikat e kriptanalizës, duke përfshirë ekzaminimin Kasiski dhe testin Friedman, të cilat ishin krijuar posaçërisht për të trajtuar shifrat polialfabetike si shifra Vigenère. Këto zbulime hapën rrugën për sulme më të rafinuara dhe një kuptim më të thellë të dobësive të kodit. Përgjatë shekullit të 20-të, përparimet në fuqinë kompjuterike dhe zhvillimi i metodave më të sofistikuara të kriptanalizës sollën në pikëpyetje sigurinë e shifrës Vigenère. Me ardhjen e kompjuterëve dixhitalë, metodat shteruese të kërkimit të çelësave u bënë më të realizueshme, duke theksuar më tej nevojën për algoritme më të forta të kriptimit. Pavarësisht ndjeshmërisë së tij ndaj teknikave moderne të kriptanalizës, shifra Vigenère ruan rëndësinë e saj historike. Ai shërben si një dëshmi e zgjuarsisë së kriptografëve të hershëm dhe kontributit të tyre në evolucionin e kriptimit. Për më tepër, sfidat e paraqitura nga shifra Vigenère stimuluan zhvillimin e algoritmeve më të fuqishme të kriptimit dhe hodhën bazat për metodat kriptografike të përdorura sot. Në seksionet vijuese të këtij punimi kërkimor, ne do të thellohemi në detajet algoritmike të shifrës Vigenère, do të eksplorojmë teknikat e tij kryesore të gjenerimit, do të analizojmë metodat e kriptanalizës të përdorura për ta thyer atë dhe do të diskutojmë konsideratat e tij të sigurisë. Duke ekzaminuar në mënyrë gjithëpërfshirëse kontekstin historik dhe aspektet teknike të shifrës Vigenère, ne mund të fitojmë një kuptim më të thellë të pikave të forta dhe të dobëta të tij, si dhe rolit të tij në formësimin e fushës së kriptografisë moderne.

# Algoritmi

Shifra Vigenère është një shifër zëvendësimi polialfabetik që funksionon në blloqe teksti të thjeshtë dhe një çelës sekret. Ai përdor alfabete të shumta zëvendësuese për të kriptuar dhe deshifruar mesazhin, duke e bërë atë më rezistent ndaj sulmeve të analizës së frekuencës.

Algoritmi i shifrës Vigenère mund të përmblidhet si më poshtë:

1. **Konfigurimi i çelësit:**
   * Çelësi i përdorur në shifrën Vigenère është një sekuencë karakteresh, zakonisht shkronja nga alfabeti.
   * Çelësi mund të zgjidhet rastësisht ose të rrjedh nga një frazë kalimi.
   * Gjatësia e çelësit është thelbësore, pasi përcakton numrin e alfabeteve të ndryshme zëvendësuese të përdorura në shifrën.
2. **Kriptimi**:
   * Teksti i thjeshtë ndahet në blloqe me gjatësi të barabartë, që zakonisht përputhet me gjatësinë e çelësit.
   * Çdo shkronjë në tekstin e thjeshtë çiftohet me një shkronjë përkatëse nga çelësi.
   * Shkronja nga çelësi përcakton alfabetin e zëvendësimit që do të përdoret për të enkriptuar shkronjën përkatëse të tekstit të thjeshtë.
   * Alfabeti i zëvendësimit merret duke zhvendosur alfabetin standard bazuar në shkronjën kryesore. Për shembull, nëse shkronja kryesore është 'B', alfabeti i zëvendësimit do të ishte alfabeti standard i zhvendosur me një pozicion.
3. **Deshifrimi:**
   * Teksti i shifruar ndahet në blloqe me gjatësi të barabartë, që përputhet me gjatësinë e çelësit.
   * Çdo shkronjë në tekstin e shifruar çiftohet me një shkronjë përkatëse nga çelësi.
   * Shkronja nga çelësi përcakton zhvendosjen e kundërt të nevojshme për të marrë shkronjën origjinale të tekstit të thjeshtë.
   * Duke aplikuar zhvendosjen e kundërt në shkronjën e tekstit të shifruar duke përdorur shkronjën kryesore, fitohet shkronja origjinale e tekstit të thjeshtë.
4. **Përsëritja e çelësit:**
   * Nëse gjatësia e tekstit të thjeshtë ose të koduar është më e gjatë se gjatësia e çelësit, çelësi përsëritet që të përputhet me gjatësinë e mesazhit.
   * Kjo përsëritje siguron që çdo shkronjë në tekstin e thjeshtë ose të shifruar të çiftohet me një shkronjë përkatëse nga çelësi.
5. **Përsëritja:**
   * Proceset e enkriptimit dhe deshifrimit kryhen në mënyrë të përsëritur për çdo bllok teksti të thjeshtë ose të koduar.
   * Rezultati është një tekst shifror ose tekst i thjeshtë që ruan strukturën e mesazhit origjinal ndërsa fsheh informacionin themelor.

# Implemetimi

Zbatimi i shifrës Vigenère përfshin përkthimin e hapave algoritmik në kod që mund të ekzekutohet në një sistem kompjuterik. Në këtë seksion, ne do të ofrojmë një analizë të konsideratave të zbatimit, aspekteve të performancës dhe kompleksitetit të shifrës Vigenère.

1. **Zgjedhja e gjuhës së programimit:**
   * Zgjedhja e gjuhës së programimit varet nga faktorë të tillë si lehtësia e përdorimit, performanca dhe disponueshmëria e bibliotekave kriptografike.
   * Gjuhët e njohura për zbatimin e shifrës Vigenère përfshijnë Python, Java, C++ dhe JavaScript.
   * Bibliotekat dhe funksionet kriptografike të disponueshme në gjuhën e zgjedhur mund të thjeshtojnë procesin e zbatimit.
2. **Përkthimi i algoritmit:**
   * Algoritmi i shifrës Vigenère, siç përshkruhet në përmbledhjen e algoritmit, duhet të përkthehet në kod.
   * Kjo përfshin hartimin e çdo hapi të algoritmit në konstruktet përkatëse të programimit, të tilla si unazat, kondicionerët dhe operacionet e vargjeve.
   * Emërtimi dhe dokumentacioni i duhur i variablave duhet të përdoren për të siguruar qartësinë dhe mirëmbajtjen e kodit.
3. **Gjenerimi kryesor:**
   * Çelësi mund të gjenerohet rastësisht ose të rrjedh nga një frazë kalimi.
   * Gjenerimi i çelësave të rastësishëm kërkon përdorimin e një gjeneruesi të përshtatshëm të numrave të rastësishëm të ofruar nga gjuha e programimit.
   * Nëse nxirret çelësi nga një frazë kalimi, një funksion i derivimit të çelësit (KDF) mund të përdoret për të kthyer frazën e kalimit në një çelës të përshtatshëm të gjatësisë së dëshiruar
4. **Konsideratat e performancës:**
   * Performanca e zbatimit të shifrave Vigenère varet nga faktorë të tillë si gjatësia e mesazhit, gjatësia e çelësit dhe efikasiteti i konstrukteve të gjuhës programuese të përdorura.
   * Kriptimi dhe deshifrimi mund të jetë intensiv nga pikëpamja llogaritëse për mesazhe të mëdha dhe çelësa të gjatë, veçanërisht në gjuhët me kohë ekzekutimi më të ngadalta.
   * Optimizimi i kujdesshëm i kodit, të tilla si minimizimi i operacioneve të tepërta dhe përdorimi i strukturave efikase të të dhënave, mund të përmirësojë performancën.
5. **Analiza e kompleksitetit:**
   * Kompleksiteti kohor i operacioneve të enkriptimit dhe deshifrimit të shifrave Vigenère është O(n), ku n është gjatësia e mesazhit ose tekstit të shifruar.
   * Kompleksiteti i hapësirës është O(1) pasi algoritmi kërkon vetëm një sasi fikse memorie shtesë për të ruajtur variablat kyç dhe të ndërmjetëm.

## Shembull implementimi

* public class VigenereCipher {
* public static String encrypt(String plaintext, String key) {
* StringBuilder ciphertext = new StringBuilder();
* int keyLength = key.length();
* for (int i = 0; i < plaintext.length(); i++) {
* char plaintextChar = plaintext.charAt(i);
* if (Character.*isLetter*(plaintextChar)) {
* char keyChar = key.charAt(i % keyLength);
* int shift = Character.*toUpperCase*(keyChar) - 'A';
* char encryptedChar = *encryptChar*(plaintextChar, shift);
* ciphertext.append(encryptedChar);
* } else {
* ciphertext.append(plaintextChar);
* }
* }
* return ciphertext.toString();
* }
* public static String decrypt(String ciphertext, String key) {
* StringBuilder plaintext = new StringBuilder();
* int keyLength = key.length();
* for (int i = 0; i < ciphertext.length(); i++) {
* char ciphertextChar = ciphertext.charAt(i);
* if (Character.*isLetter*(ciphertextChar)) {
* char keyChar = key.charAt(i % keyLength);
* int shift = Character.*toUpperCase*(keyChar) - 'A';
* char decryptedChar = *decryptChar*(ciphertextChar, shift);
* plaintext.append(decryptedChar);
* } else {
* plaintext.append(ciphertextChar);
* }
* }
* return plaintext.toString();
* }
* private static char encryptChar(char c, int shift) {
* if (Character.*isUpperCase*(c)) {
* return (char) ((c - 'A' + shift) % 26 + 'A');
* } else {
* return (char) ((c - 'a' + shift) % 26 + 'a');
* }
* }
* private static char decryptChar(char c, int shift) {
* if (Character.*isUpperCase*(c)) {
* return (char) ((c - 'A' - shift + 26) % 26 + 'A');
* } else {
* return (char) ((c - 'a' - shift + 26) % 26 + 'a');
* }
* }
* public static void main(String[] args) {
* String plaintext = "Hello, World!";
* String key = "KEY";
* String encryptedText = *encrypt*(plaintext, key);
* System.***out***.println("Encrypted text: " + encryptedText);
* String decryptedText = *decrypt*(encryptedText, key);
* System.***out***.println("Decrypted text: " + decryptedText);

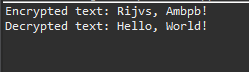
## Dokumentimi I kodit:

Ky kod zbaton shifrën Vigenere, një shifër zëvendësimi polialfabetik që kodon dhe deshifron tekstin duke përdorur një fjalë kyçe. Këtu është një dokumentacion i shkurtër i kodit: Klasa VigenereCipher ofron dy metoda kryesore: enkriptimin dhe dekriptimin, të cilat marrin një tekst të thjeshtë ose të shifruar dhe një çelës si hyrje dhe kthejnë përkatësisht tekstin shifror ose tekstin e thjeshtë. Metoda e enkriptimit merr një varg teksti të thjeshtë dhe një varg çelësi si parametra. Ai përsëritet mbi çdo karakter në tekstin e thjeshtë dhe kryen procesin e kriptimit. Nëse karakteri është një shkronjë, ai përcakton karakterin përkatës të çelësit bazuar në gjatësinë e çelësit dhe pozicionin aktual. Më pas llogarit vlerën e zhvendosjes duke konvertuar karakterin kryesor në shkronja të mëdha dhe duke zbritur 'A'. Metoda përdor funksionin ndihmës encryptChar për të zhvendosur karakterin e tekstit të thjeshtë me vlerën e llogaritur të zhvendosjes dhe shton karakterin e koduar në një StringBuilder të quajtur ciphertext. Nëse karakteri nuk është një shkronjë, ai e shton atë në tekstin e shifruar pa kriptim. Së fundi, ai e kthen tekstin e koduar si një varg. Metoda e dekriptimit është e ngjashme me metodën e enkriptimit, por ajo kryen procesin e deshifrimit. Ai merr një varg teksti të koduar dhe një varg çelësi si parametra. Ai përsëritet mbi çdo karakter në tekstin e shifruar, përcakton karakterin përkatës të çelësit bazuar në gjatësinë e çelësit dhe pozicionin aktual dhe llogarit vlerën e zhvendosjes. Metoda përdor funksionin ndihmës decryptChar për të zhvendosur karakterin e tekstit të shifruar me vlerën e llogaritur të zhvendosjes dhe shton karakterin e deshifruar në një StringBuilder të quajtur plaintext. Nëse karakteri nuk është një shkronjë, ai e shton atë në tekstin e thjeshtë pa deshifrim. Së fundi, ai e kthen tekstin e deshifruar si një varg. Funksioni ndihmës encryptChar merr një karakter c dhe një zhvendosje të numrit të plotë si parametra dhe kryen enkriptimin për një karakter të vetëm. Kontrollon nëse karakteri është i madh ose i vogël dhe zbaton funksionin e ndërrimit në përputhje me rrethanat, duke e mbështjellë rreth alfabetit nëse është e nevojshme. Ai kthen karakterin e koduar. Funksioni ndihmës decryptChar është i ngjashëm me encryptChar, por kryen deshifrimin për një karakter të vetëm. Kontrollon gjithashtu nëse karakteri është i madh ose i vogël, zbaton funksionin e ndërrimit dhe mbështillet rreth alfabetit nëse është e nevojshme. Ai kthen karakterin e deshifruar.

Në metodën kryesore, një shembull i tekstit të thjeshtë "Përshëndetje, Botë!" dhe një çelës "KEY" janë dhënë. Ai thërret metodën e enkriptimit për të enkriptuar tekstin e thjeshtë duke përdorur çelësin dhe printon tekstin e koduar. Më pas, ai thërret metodën e dekriptimit për të deshifruar tekstin e koduar duke përdorur të njëjtin çelës dhe printon tekstin e deshifruar.

## Rezultati:

}



# Konkluzioni

Shifra Vigenère, me futjen e tij të zëvendësimit polialfabetik, luajti një rol kryesor në zhvillimin historik të teknikave të kriptimit. Ai ofroi një përmirësim të rëndësishëm në krahasim me shifrat e mëparshme duke futur ndryshueshmëri në modelin e zëvendësimit bazuar në një çelës sekret. Pavarësisht ndjeshmërisë së tij ndaj sulmeve të njohura me tekst të thjeshtë dhe ardhjes së teknikave më të avancuara të kriptanalizës, shifra Vigenère mbetet një mjet i vlefshëm për të kuptuar evolucionin e kriptografisë. Nëpërmjet këtij punimi kërkimor, ne kemi eksploruar sfondin historik, detajet algoritmike dhe konsideratat e zbatimit të shifrës Vigenère. Ne kemi ekzaminuar pikat e tij të forta, të tilla si rezistenca ndaj sulmeve të analizës së frekuencës, dhe dobësitë e tij, të tilla si cenueshmëria ndaj sulmeve me tekst të njohur. Duke studiuar shifrën Vigenère, studiuesit mund të fitojnë njohuri mbi sfidat me të cilat përballen kriptografët e hershëm dhe të vlerësojnë themelet që ata hodhën për algoritmet moderne të kriptimit. Ndërsa shifra Vigenère mund të mos ofrojë nivelin e sigurisë që kërkohet në aplikacionet kriptografike bashkëkohore, ai vazhdon të shërbejë si një referencë edukative dhe historike. Kompleksitetet dhe dobësitë e tij i kanë shtyrë kriptanalistët të zhvillojnë metoda më të sofistikuara, duke kontribuar në avancimin e teknikave të kriptimit. Ndërsa teknologjia evoluon, algoritmet e kriptimit duhet të përshtaten për të adresuar kërcënimet në zhvillim dhe për të siguruar konfidencialitetin e informacionit të ndjeshëm. Ndërsa shifra Vigenère mund të mos jetë e përshtatshme për aplikime moderne që kërkojnë garanci të forta sigurie, rëndësia e tij historike nuk mund të anashkalohet. Shifra shërben si një kujtesë për garën e vazhdueshme të armëve midis kriptografëve dhe kriptanalistëve dhe thekson nevojën për inovacion të vazhdueshëm në fushën e kriptografisë. Duke studiuar shifrën Vigenère, studiuesit fitojnë një kuptim më të thellë të parimeve të kriptimit, dizajnit të algoritmit dhe rëndësisë së menaxhimit të çelësave. Kjo njohuri mund të informojë zhvillimin e algoritmeve të fuqishme të kriptimit dhe protokolleve kriptografike që i rezistojnë sulmeve moderne dhe mbrojnë të dhënat e ndjeshme në një botë gjithnjë e më të ndërlidhur. Si përfundim, shifra Vigenère qëndron si një testament për zgjuarsinë dhe këmbënguljen e kriptografëve të hershëm. Duke shqyrtuar kontekstin e tij historik, detajet algoritmike dhe konsideratat e zbatimit, ne zgjerojmë të kuptuarit tonë për evolucionin e kriptografisë dhe sfidat me të cilat përballemi në ndjekjen e komunikimit të sigurt. Nëpërmjet kërkimit dhe inovacionit të mëtejshëm, ne mund të vazhdojmë të ndërtojmë mësimet e nxjerra nga shifra Vigenère për të zhvilluar teknika të avancuara të enkriptimit që plotësojnë kërkesat e sigurisë të epokës sonë dixhitale.